Task 2 PRF

```
def g0(k):
    new_k = task1.g_calc(k)
    # print("g0:", new_k)
    return new_k[:len(k)]


def g1(k):
    new_k = task1.g_calc(k)
    # print("g1:", new_k)
    return new_k[len(new_k)//2:len(new_k)//2+len(k)]
```

G0

Function is called when the input string being iterated over encounters digit 0. It calls PRG created in task1 and from the bit string of length 2*x returned, it returns the first x bits to the calling function.

G1

Function is called when the input string being iterated over encounters digit 1. It calls PRG created in task1 and from the bit string of length 2*x returned, it returns the last x bits to the calling function.

```
def xor(a, b):
    min_length = min(len(a), len(b))
    xor_message = ""
    for i in range(min_length):
        if a[i] == b[i]:
            xor_message += "0"
        else:
            xor_message += "1"

    return xor_message
```

\

Xor()

Calculates and returns the xor value of the 2 bit strings provided as input.

```
def pseduoRandFunc(key, input):
    # r = task1.g_calc(seed)[:len(message)]
    # print(r)
    encr = key
    for i in input:
        # print(encr)
        if i == '0':
            encr = g0(encr)
        else:
            encr = g1(encr)

    # print("Enc ", encr)

    # encr = xor(encr, message)
    return encr
```

pseudoRandFunc()

Driver function of the task takes key and input from user (both in binary). Here, the function iterates over the message provided as input and calls the respective function based on the encountered bit.

Sample Input

Key: 10011

Message : 11111

Sample Output

11101